

Amendments to the Claims:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A control method of an Internet facsimile being connected to a telephone network and Internet for transferring electronic mail received via the Internet by facsimile, the control method comprising the steps of:

receiving electronic mail containing an ~~password-encrypted~~ encrypted password ~~and related-relating~~ to a control command for indicating a facsimile communication function;

decrypting the ~~password-encrypted~~ encrypted password; and

transferring an electronic mail document by facsimile following the control command using the ~~password-decrypt~~ decrypted password.

2. (Original) The control method as claimed in claim 1 wherein the password is encrypted and set in a main body of the electronic mail.

3. (Original) The control method as claimed in claim 1 wherein the password is encrypted and set in a destination field of received electronic mail.

4. (Original) The control method as claimed in claim 1 wherein the encryption of the password is performed in an encryption system of S/MIME (Secure/Multipurpose Internet Mail Extension) or PGP/MIME (Pretty Good Privacy/ Multipurpose Internet Mail Extension).

5. (Original) The control method as claimed in claim 1 wherein the control command indicates a confidential communication function, a bulletin board communication function, or a relay broadcast communication function defined in ITU-T (International Telecommunications Union-Telecommunications Standards Section) Recommendation T.30.

6. (Currently Amended) An Internet facsimile being connected to a telephone network and Internet and having a function of transferring an electronic mail document received via the Internet by facsimile, the Internet facsimile comprising:

a determination section, upon reception of an electronic mail document to be transferred by facsimile, for determining whether or not a password related to a control command for indicating a facsimile communication function is encrypted and set in the electronic mail;

a decryption section for decrypting the password if the determination section determines that the electronic mail has the ~~password encrypted~~ encrypted password; and

a communication control section for transferring the electronic mail by facsimile following the control command using the decrypted password.

7. (Original) The Internet facsimile as claimed in claim 6 wherein if the determination section determines that the password is encrypted in a main body of the received electronic mail, the decryption section decrypts the encrypted password.

8. (Original) The Internet facsimile as claimed in claim 6 wherein if the determination section determines that the password is encrypted in a destination field of the received electronic mail, the decryption section decrypts the encrypted password.

9. (Original) The Internet facsimile as claimed in claim 6 wherein the password is encrypted according to an encryption system of S/MIME (Secure/Multipurpose Internet Mail Extension) or PGP/MIME (Pretty Good Privacy/ Multipurpose Internet Mail Extension).

10. (Original) The Internet facsimile as claimed in claim 6 wherein the control command indicates a confidential communication function, a bulletin board communication function, or a relay broadcast communication function defined in ITU-T (International Telecommunications Union-Telecommunications Standards Section) Recommendation T.30.

11. (Currently Amended) A communication instruction terminal having a function of instructing an Internet facsimile to transfer an electronic mail by facsimile through Internet, the communication instruction terminal comprising:

an encryption section for encrypting a password related to a control ~~command~~ command, wherein the control command is for indicating a facsimile communication function and the encrypted password is added to the electronic mail to be transferred by facsimile by an encryption system for encrypting the electronic mail; facsimile; and

a sending section for giving the password encrypted by the encryption section to the electronic mail and sending the electronic mail.

12. (Original) The communication instruction terminal as claimed in claim 11 wherein the sending section sets the encrypted password in a destination field of the electronic mail.

13. (Original) The communication instruction terminal as claimed in claim 11 wherein the sending section sets the encrypted password in a main body of the electronic mail.

14. (Original) The communication instruction terminal as claimed in claim 11 wherein the encryption section encrypts the password using an encryption system of S/MIME (Secure/Multipurpose Internet Mail Extension) or PGP/MIME (Pretty Good Privacy/Multipurpose Internet Mail Extension).

15. (Original) The communication instruction terminal as claimed in claim 11 wherein the control command indicates a confidential communication function, a bulletin board communication function, or a relay broadcast communication function defined in ITU-T (International Telecommunications Union-Telecommunications Standards Section) Recommendation T.30.

16. (Currently Amended) An Internet facsimile being connected to both a telephone network and Internet and having a function of transferring an electronic mail document received via the Internet by facsimile, the Internet facsimile comprising:

a determination section, upon reception of an electronic mail document to be transferred by facsimile, for determining whether or not the transmission source is identified correctly; and

a communication control section for transferring the received electronic mail by facsimile over the telephone network only if the determination section determines that the transmission source is identified correctly.

17. (Original) The Internet facsimile as claimed in claim 16 wherein the determination section uses a function of S/MIME (Secure/Multipurpose Internet Mail Extension) or PGP/MIME (Pretty Good Privacy/ Multipurpose Internet Mail Extension) to determine whether or not the transmission source can be identified correctly.